

Below are a variety of HIPAA Topics that may be of interest.

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Have a great day!!!
Ken

Topics included below are:

AHIMA Information

CALINX Information

Claredi - HIPAA Transactions Testing Service Goes Live

WEDI-SNIP Testing paper and information available

[hipaalive] Re: GENERAL: HIPAA COSTS/FUNDING LEVELS

[hipaalert] One Week until the First Legally HIPAA! Audioconference, June 20th

[hipaalive] Privacy- Gramm-Leach vs HIPAA

[hipaalive] RE: SECURITY: Sending Member Information via E-Mails

[hipaalive] Re: Definition PHI (was PRIVACY)

CNN: HHS secretary announces changes to HCFA

[hipaalive] RE: TCS: Hybrid Entity and TCS Rules

[hipaalive] RE: PRIVACY: Role-based access

[hipaalive] RE: General: HIPAA Privacy Regulation and Federal Sub Abuse Regulation

***** AHIMA Information *****

The American Health Information Management Association (AHIMA) has a wide variety of information and articles on HIPAA. Some can be found at:

www.ahima.org/journal/index.html In the near future they may have a variety of articles and proceeds from their recent Conference on the Website, so it may be a good website to monitor.

***** CALINX Information *****

The California Information Exchange has a variety of HIPAA information that you may find interesting at:

www.calinx.org/

Try also their resources references at <http://www.calinx.org/resources.asp>

>>> Sharon Winsberg 06/12/01 11:08AM >>>

I found this information and I am sending it on to you for distributions if you think this is something folks would like to know about, if they don't already.

HIPAA Transactions Testing Service Goes Live

(June 01, 2001) Claredi has launched the production version of a Web site to test the HIPAA compliance of administrative transactions. The Salt Lake City-based vendor this spring offered services on the site, www.claredi.com in a testing phase.

The site tests all data elements and structural components of HIPAA-mandated ANSI 837 institutional, professional and dental claims transactions to six levels recommended by the Workgroup for Electronic Data Interchange, Reston, Va. It also tests for a proprietary trading partner-specific seventh level. Full testing of all other HIPAA transactions up to WEDI levels 1 and 2 also are available; Claredi will complete its development of the additional transactions testing services by the fourth quarter. Additional information on the various testing levels is available under the Frequently Asked Questions section of the Web site.

Claredi offers third-party certification that a health care organization's transactions comply with the implementation guides that govern HIPAA-mandated transactions. Provider organizations, payers and claims clearinghouses developing HIPAA-compliant transactions can use the Web site on a subscription basis to test compliance with portions of a transaction, or all of it. Even if an organization is not ready for certification, using the Web site's testing software can provide a line-by-line roadmap to follow in making necessary modifications during development, says Kepa Zubeldia, Claredi's CEO.

***** WEDI-SNIP Info - Testing

For WEDI-SNIP Testing info go to:

<http://www.wedi.org/snip/Transactions/Testing000105.pdf>

Other info at WEDI-SNIP Site has Implementation Assistance information on:

- Transactions and Code Sets
- Identifiers
- Security and Electronic Signatures
- Privacy
- Checklists
- Electronic Medical Records
- Dental

Go to the address: http://www.wedi.org/snip/snip_implem.htm for more info.

Their current info on Transactions and Code Sets includes the text below and is at:

http://www.wedi.org/snip/implementation/transactions_code_sets.html

Transactions and Code Sets

SNIP -- Transactions Work Group White Papers

(These documents are .pdf files, you will need Adobe® Acrobat® Reader™ to view. If you do

not have Adobe® Acrobat® Reader™, please click here to download.)

Data and Code Set Compliance - DRAFT-For discussion only

Trading Partner Agreements- DRAFT-For discussion only

Impact on DDE Services - DRAFT-For discussion only

Testing and Certification - - DRAFT-For discussion only

Business-to-Business Transaction Set Testing - DRAFT-For discussion only

Sequencing Proposal

Provider Taxonomy Codes

These codes identify and code provider type and provider area of specialization for all medical related providers.

Provider Taxonomy to Specialty Code Crosswalk

This file contains taxonomy codes cross walked with HCFA specialty codes. The Translations

sub-workgroup is looking for people to help determine the completeness and accuracy of this

document. Comments may be sent to Mark McLaughlin,

Mark.McLaughlin@itb.mckhboc.com,

or Catherine Schulten, Catherine.Schulten@neonsoft.com. Members of the Translations listserv

can send comments directly to the listserv at translations@wedi.org.

Remark codes

Remark codes must be used to relay service-specific informational messages that cannot be

expressed with a reason code. Remark codes are maintained by the Health Care Financing

Administration (HCFA) but may be used by any health care payer when they apply.

Adjustment status codes

Adjustment status code crosswalk guide

This document is intended to assist payers in creating crosswalks from their internal edits to

claim status (277) codes.

FAQ on the HCFA 1500 form developed by the National Uniform Claim Committee

AFEHCT- HCFA 1500/837 Print Images & HIPAA Demonstration Project

The computerized "image" of the paper HCFA-1500 and UB92 forms are widely used as input

mechanisms to systems for the generation of electronic claims. However, the X12 4010 837

Implementation Guides call for significantly more data than is on these forms. The National

Uniform Claim Committee (NUCC) is concerned about the data content of the HCFA-1500 form in this context.

AFEHCT has voted to work with NUCC on a demonstration project and resulting analysis of the issue. In addition, AFEHCT would like to perform this demonstration and analysis on institutional (UB92) claims.

To do this work, AFEHCT has established the Print Images & HIPAA Demonstration Project. The

prime objective of this project is to demonstrate and provide a thorough analysis of the methods

and viability of continuing the use of the HCFA-1500 and UB92 data sets in the generation of

HIPAA-compliant electronic claims in a real-life environment. Some areas of concern that have

been identified concerning the migration to the 837 from the HCFA 1500 / UB92 have been

identified.

Designated Standard Maintenance Organizations
The Standards for Electronic Transactions HIPAA rule establishes a new category of organization, the "Designated Standard Maintenance Organization (DSMO)." Section 162.910 of this final regulation provides that the Secretary may designate as DSMOs those organizations that agree to maintain the standards adopted of the Secretary. Section 162.910 also establishes criteria for the processes to be used in such maintenance. Several Data Content Committees (DCCs) and Standard Setting Organizations (SSOs) have agreed to maintain those standards designated as national standards in the final rule "Standards for Electronic Transactions" according to the criteria established by the Secretary.

***** [hipaalive] Re: GENERAL: HIPAA COSTS/FUNDING LEVELS

Blue Cross Commissioned this study of Privacy legislation Costs:
http://www.privacysecuritynetwork.com/healthnews/features_costsest212.cfm

http://www.privacysecuritynetwork.com/healthnews/features_costsest212.cfm

Costs Estimates for HIPAA Privacy
Proposal & Leading Congressional
Proposals

Cost Estimates for HHS's HIPAA Medical Privacy
Proposed Regulation
HHS's estimate of the costs to business imposed by its
medical privacy proposal.

Cost Estimates for the Leading Congressional Medical
Privacy Legislative Proposals
The Blue Cross/Blue Shield Association's estimate of the
cost to business that would be imposed by the leading
congressional proposals on medical privacy.

***** [hipaalert] One Week until the First Legally HIPAA! Audioconference, June 20th

Order one or all three sessions at our new HIPAAstore!
<http://www.hipaadvisory.com/ezcart/>

>>> LEGALLY HIPAA! A Special Summer Audioconference Series <<<

June 20 -- Handling Consents and Authorizations
July 18 -- Handling Chain of Trust and Business Associate Agreements
Aug 22 -- Developing Security/Privacy Policies and Procedures

From: Phoenix Health Systems, publishers of HIPAAAdvisory.com,
"the HIPAA hub of the Web" (Modern Healthcare)

DON'T MISS YOUR CHANCE TO TUNE IN TO HIPAAALERT's legal HIPAAAdvisor, Steve Fox, Esq -- as he identifies and clarifies HIPAA's central legal issues. An engaging, nationally prominent speaker and prolific author on HIPAA and healthcare information technology issues, Steve and his "supporting cast" will simplify the complex in down-to-earth English and a minimum of "legalese." Steve's most recent speaking engagements include ACHE 2001, HIMSS 2001, the American Health Lawyers Association, and various state HFMA and HIMSS groups. SIGN UP TODAY at <http://www.hipaadvisory.com/order/legal/>

WHAT WE WILL COVER:

SESSION 1 -- Handling Consents and Authorizations

- How Does the Privacy Rule Affect Access to Health Information?
- Information Uses and Disclosure -- What is the Impact of the Privacy Rule on Access to Care, Marketing, Fundraising, and Research?
- What Are the Differences between Patient Consent and Authorization?
- When May a Patient be Treated without Giving Consent?
- What Activities may be Engaged in Only after Patient Authorization?
- How Do I Implement Consent/Authorization Policies and Forms?

SESSION 2 -- Handling Chain of Trust and Business Associate Agreements

- Who Are My Business Associates under HIPAA?
- How are these Relationships Defined and Differentiated?
- What are Their Key Components -- Including Required Terms and Conditions?
- How Do I Implement Chain of Trust and Business Associate Agreements?
- How Do I Manage These Relationships?

SESSION 3 -- Developing Security/Privacy Policies and Procedures

- What Policies and Procedures does HIPAA Require?
 - Who is Affected and How?
 - What Are the Components of Compliant, Effective Policies and Procedures?
 - How Do I Evaluate Current Policies and Procedures?
 - How Do I Implement Security/Privacy Policies and Procedures?
-

FACULTY:

PRINCIPLE SPEAKER: Steve Fox, Esq., HIPAAAlert's legal HIPAAAdvisor -- Partner & Healthcare Informatics Practice Leader of Pepper Hamilton LLP, Washington DC. -- JOINED BY: Rachel Wilson, Esq., Associate with Pepper Hamilton LLP, PLUS members of Phoenix' HIPAA Solutions Team

WHO WILL BENEFIT?

For healthcare leaders and professionals involved in HIPAA Privacy and Security compliance. For COO's, CIO's, Compliance Officers, Privacy Officers, HIPAA Steering Committee members, Medical Directors, Physicians, Department Heads, Legal Staff, MIS Staff.

WHEN?

60-minute AudioConferences:
Wednesday, June 20, 2001, 2:00-3:00 p.m. (EDT)
Wednesday, July 18, 2001, 2:00-3:00 p.m. (EDT)
Wednesday, August 22, 2001, 2:00-3:00 p.m. (EDT)

PRICING:

\$130 for each live Legally HIPAA! AudioConference, including complete program materials. As always, feel free to invite your office associates to join you in listening in on your call.

SIGN UP TODAY!!

GO TO <http://www.hipaadvisory.com/ezcart/>

SPONSORED BY -- Phoenix Health Systems, publishers of HIPAAAlert and HIPAAAdvisory.com, "the HIPAA hub of the Web" (Modern Healthcare, 10/2000)

Questions? E-mail us at info@phoenixhealth.com

FORWARD this posting to interested associates, who may subscribe free to HIPAAAlert at:

<http://www.hipaadvisory.com/alert/>

Subscribe to our free discussion list at:

<http://www.hipaadvisory.com/live/>

Get a weekly byte of HIPAA at:

<http://www.hipaadvisory.com/notes/>

You are currently subscribed to hipaaalert as:kmckinst@dmhhq.state.ca.us

To unsubscribe send a blank email to leave-hipaaalert-85079900@lists.hipaalert.com

***** [hipaalive] Privacy- Gramm-Leach vs HIPAA

*** This is HIPAAlive! From Phoenix Health Systems ***

A health plan is included in the Gramm Leach Bliley Act; effective July 1, 2001. You will need to send a Notice of Privacy to each of your members, just as we are doing, at least once a year.

In Florida, as long as you are progressing toward HIPAA compliance on privacy then you are compliant with GLB but you'll have to check with your legislature in Tennessee for yourself.

Hope this helps.

Charlene A. Dickerson
Project Manager
Physicians Healthcare Plans, Inc.
1410 N. Westshore Blvd., Suite 200
Tampa, FL 33607

*** This is HIPAAlive! From Phoenix Health Systems ***

Hi Scott,
I have to take exception with your comment about HMOs. The lawyers (and there were many) part of in-house and outside counsel felt that the HMO pieces of this large insurance company were also covered under GLB.

One other notes for you GLBers, the NIAA model is a good starting point and you can find that on the net. Also, if you are compliant with HIPAA, then you are compliant with GLB, according to that model. However, GLB deadline is much sooner, obviously.

Miriam Paramore
PCI

*** This is HIPAAlive! From Phoenix Health Systems ***

Most of the states I am familiar with DO consider HMOs a financial institution as defined by GLBA and therefore subject to the notice requirements. As GLBA defines financial institutions very broadly, many states believe it appropriate to include HMOs. See the definition of financial activates for additional details.

Jeff Schneewind
Compliance Officer
Definity Health

*** This is HIPAAlive! From Phoenix Health Systems ***

In California, the Department of Managed Healthcare has determined that "Knox-Keene licensed health care service plans do not fall within the scope of insurers governed by the GLB Act.. Therefore, the GLB Act is not applicable to Knox-Keene licensees." Other states may see things differently.

Tracy Azevedo
UCDavis Health System

e-mail: tracy.azevedo@ucdmc.ucdavis.edu

***** [hipaalive] RE: SECURITY: Sending Member Information via E-Mails

*** This is HIPAAlive! From Phoenix Health Systems ***

Hello Steven,

The proposed security rule states at §142.308(d)(1)(ii) that you must employ either network access controls or encryption. Since the information that you transmit will likely traverse network components over which you have no control, network access controls are not an option. There are several email encryption products on the market but you would have to somehow coordinate the installation of compatible software among all potential recipients. For most organizations, this would impose an administrative burden that would far outweigh any benefit that you hoped to receive.

Your best bet would be to incorporate a messaging system into your web site that members and providers would access over an SSL connection. You could send a generic "check your messages" note by regular email whenever a communication was initiated on your end. The sensitive data would subsequently be transmitted over an encrypted SSL link. (Just about everyone has this capability built into the browser software that they use, and it requires no manual intervention.)

Bye for now -- Harry

Harry E. Smith, CISSP
Timberline Technologies LLC

*** This is HIPAAlive! From Phoenix Health Systems ***

In my opinion...

Yes, the information would need to be encrypted based on my interpretation of the current HIPAA regulations.

Second, even if the regulations do not require encryption, please consider unencrypted email sent via the internet to be much the same as a postcard. As a practical matter, consider how little information you would (or even should) put on a postcard for prying eyes to see.

One person's opinion

Brian J. Duane
Duane Consulting

***** [hipaalive] Re: Definition PHI (was PRIVACY)

*** This is HIPAAlive! From Phoenix Health Systems ***

Yes - once Individually Identifiable Health Information becomes Protected Health Information, then all PHI is controlled under HIPAA. This includes subsets of the PHI which may be identifiable, but may not necessarily directly contain related health information. Unless it is a disclosure for a purpose for which consent or authorization is not required, disclosure of PHI that individual permission is not given through consent, right to agree or object, or authorization is prohibited.

See Page 82804 for the definition of Individually Identifiable Health Information - Note "including demographic information" and 2(ii).

Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

- (1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 - (i) That identifies the individual; or
 - (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

See Page 82805 for a definition of Protected Health Information

Protected health information means individually identifiable health information:

- (1) Except as provided in paragraph (2) of this definition, that is:
 - (i) Transmitted by electronic media;
 - (ii) Maintained in any medium described in the definition of electronic media at § 162.103 of this subchapter; or
 - (iii) Transmitted or maintained in any other form or medium.
- (2) Protected health information excludes individually identifiable health information in:
 - (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and
 - (ii) Records described at 20 U.S.C. and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Also See Sec. 164.514(b) for a list of elements that are considered identifiable regarding 2(i) above.

Implementation specifications: requirements for de-identification of

protected health information.

A covered entity may determine that health information is not individually identifiable health information only if:

(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except

for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

NOTE: You can also release components of PHI if a person with appropriate statistical knowledge, using generally accepted statistical principals and scientific methods, determines that the information (alone or in combination with other information) to be released to a particular recipient has a very low risk of re-identification. Of course the methods and results have to be documented.

I hope this helps,
Thanks,
Tom Hanks
37W542 High Point Court
St. Charles, IL 60175

***** CNN: HHS secretary announces changes to HCFA

HHS secretary announces changes to HCFA

June 15, 2001 Posted: 8:24 AM EDT (1224 GMT)

WASHINGTON (CNN) -- The Health Care Financing Administration (HCFA), the government agency that oversees Medicare and Medicaid, will change its name to the Centers for Medicare and Medicaid Services, Health and Human Services Secretary Tommy Thompson announced Thursday.

The change is part of the first in a series of reforms designed to strengthen services at the \$400 billion agency.

"We're making quality service the number one priority in this agency," Thompson said. "These sweeping reforms will strengthen our programs and enable our dedicated employees to better serve Medicare and Medicaid beneficiaries as well as health care providers.

"We're going to encourage innovation, better educate consumers about their options and be more responsive to the health care needs of Americans."

The Centers for Medicare and Medicaid Services will include three centers:

-- The Center for Beneficiary Choices will focus on the choices Medicare beneficiaries have under the Medicare, Medigap and Medicare + Choice programs. Medicare + Choice provides for options outside the traditional fee-for-service program, such as HMOs.

-- The Center for Medicare Management will work with the traditional fee-for-service Medicare.

-- The Center for Medicaid and State Operations will focus on programs administered by states, including Medicaid and the State Children's Health Insurance Program (SCHIP). A person will be assigned to work directly with each state.

The agency will be kicking off a national media campaign this fall to educate beneficiaries and help them better understand the choices they have under Medicare. And it will work towards reforming its relationship with private companies that process and pay fee-for-service Medicare claims.

Thompson said the restructured agency would renew efforts to reach out to patients and providers.

highest "This is only the beginning -- more changes are on the way," he said. "We're going to keep fine-tuning this department so Americans are receiving the quality health care possible. Our commitment to excellence is unwavering."

Last year there were 70 million Medicare, Medicaid and SCHIP beneficiaries.

While the new name is effective immediately, it will be phased in over time on letterhead, signs, and other places where HCFA is currently listed.

***** [hipaalive] RE: TCS: Hybrid Entity and TCS Rules

*** This is HIPAAlive! From Phoenix Health Systems ***

With a hybrid entity, any of their health care components that would be a covered entity under HIPAA if they stood alone, are treated as a covered entity under HIPAA.

- 1) If the main entity would not be a covered entity under HIPAA, they are not a covered component of the hybrid entity.
- 2) However, there has to be a firewall between the covered components and the non-covered components to protect the PHI.
- 3) Even if the main entity is not a covered entity, they are probably the responsible entity.

Note: If most of the activities of a hybrid entity are related to health care, then the entire entity and all of its components are treated as a covered entity.

See FR 82502 for a discussion of hybrid entities.

Thanks,

Tom Hanks
37W542 High Point Court
St. Charles, IL 60175

***** [hipaalive] RE: PRIVACY: Role-based access

*** This is HIPAAlive! From Phoenix Health Systems ***

Sure,

Here are some resources for Role Based Access Control (RBAC).

1) SANS Institute has a good basic primer on RBAC

<http://www.sans.org/infosecFAQ/securitybasics/RBAC.htm>

Also go to their home page for a complete list of very good security resources <http://www.sans.org/newlook/home.htm>

2) NIST Draft standard for Role Based Access Control:

<http://csrc.nist.gov/rbac/>

3) Paper on RBAC for clinical records - note the study was done in Greece and follows a stricter European model:

<http://www.ics.forth.gr/ICS/acti/cmihta/publications/papers/2000/mie2000/mie2000.html>

4) This is a very brief outline of RBAC - Australian - but the site has a number of other security resources that may be helpful

<http://security.dstc.edu.au/projects/access/RBAC.html>

5) Very nice presentation of health care oriented RBAC:

<http://www.mcs.vuw.ac.nz/courses/COMP413/2001/LectureNotes/9.AccessControl/index.htm>

6) Download a paper on an Interoperable RBAC Model from Univ. of IL Computer Science - very interesting multi-domain model a little technical, but a good primer on establishing a mathematical model:

<http://www.mcs.vuw.ac.nz/courses/COMP413/2001/LectureNotes/9.AccessControl/index.htm>

7) Download - Although this is a commercial site - it is a very good paper (developer level) from HP Labs describing integration of policy based RBAC with Common Data Security Architecture for Internet based application access -

<http://www.hpl.hp.com/techreports/1999/HPL-1999-59.html>

Most of the operating system vendor sites also have documentation on implementing RBAC (e.g. Solaris, Novell, Microsoft (NT, 2000, IIS & TS))

I hope this helps,

Thanks,

Tom Hanks
37W542 High Point Court
St. Charles, IL 60175

***** [hipaalive] RE: General: HIPAA Privacy Regulation and Federal Sub Abuse Regulation *****

Go to www.access.gpo.gov/nara/cfr/waisidx_98/42cfr2_98.html

<http://www.access.gpo.gov/nara/cfr/waisidx_98/42cfr2_98.html> and you

will find the table contents to Confidentiality of Alcohol and Drug Abuse Patient Records.

Rick
Rick Ensenbach CISA, CISSP
Director, Healthcare Security Services
InterSec Communications, Inc.

*** This is HIPAAlive! From Phoenix Health Systems ***

No you do not need to have two sets of policies.

The HIPAA rules are a floor. Any state law, federal law, or your own internal policy that sets a higher standard will satisfy HIPAA.

A conservative approach would be to document that you have reviewed your existing relevant policies and (a) upgraded those that are found to not meet HIPAA requirements, (b) developed new policy and procedures where necessary, and (c) have confirmed that existing policy and procedures meet or exceed HIPAA.

-----Original Message-----

From: YONGGANG ZENG [<mailto:YONGGANG@huroncmh.org>]

Sent: Thursday, June 14, 2001 11:53 AM

To: HIPAAlive Discussion List

Subject: [hipaalive] General: HIPAA Privacy Regulation and Federal Sub Abuse Regulation